(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 July 2003 (31.07.2003)

PCT

(10) International Publication Number
WO 03/063431 A2

(51) International Patent Classification[7]: H04L 12/58, 29/06

(21) International Application Number: PCT/EP03/00752

(22) International Filing Date: 23 January 2003 (23.01.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0201648.3 25 January 2002 (25.01.2002) GB

(71) Applicant *(for all designated States except US)*: **F-SECURE OYJ** [FI/FI]; Tammasaarankatu 7, PL 24, Helsinki, FIN-00180 Helsinki (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LAHTI, Pasi** [FI/FI]; Stuurenkatu 5 A 20, FIN-00510 Helsinki (FI).

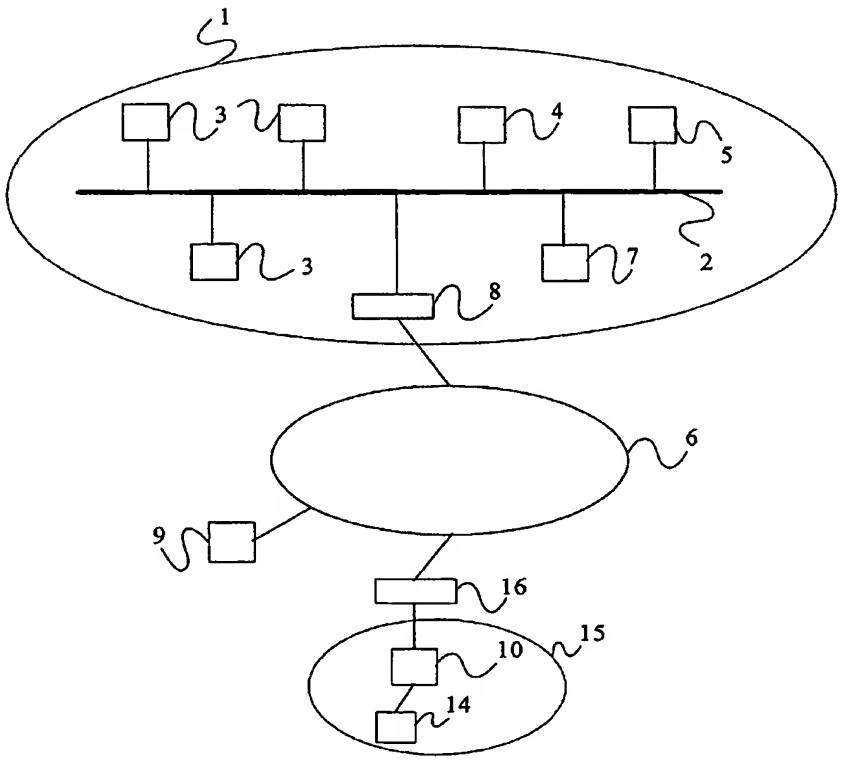
(74) Agents: **MARKS & CLERK** et al.; 4220 Nash Court, Oxford Business Park South, Oxford, Oxfordshire OX4 2RU (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: ANTI-VIRUS PROTECTION AT A NETWORK GATEWAY



(57) Abstract: A method of preventing the infection of a computer network 1 by a computer virus, where that virus can be spread by e-mail traffic. The method comprises installing at an e-mail gateway 7 of the network an anti-virus application 12, which application scans at least incoming e-mail traffic for known viruses. In the event that a new virus is detected by the provider of the anti-virus application 12, a notification of this event is sent from the provider to the anti-virus-application 12. At the anti-virus application 12, receipt of said notification results in the diversion of incoming e-mails or their attachments to a buffer 13 for safe storage.

WO 03/063431 A2

Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Anti-Virus Protection at a Network Gateway

Field of the Invention

The present invention relates to the provision of anti-virus protection at a network gateway.

Background to the Invention

Much damage has recently been caused by the creation and spread of software viruses. As well as the loss and corruption of data, viruses have been responsible for the shutting down of individual computers and even entire networks, leading to a great loss in productivity. The recent "success" of software viruses such as the "Love Letter" virus is due to the proliferation of e-mail as a means of communication between computer users coupled with a lack of knowledge of the potential problems amongst computer users (e.g. users will open e-mail attachments without regard to their origins).

In order to mitigate the potential damage caused by viruses, responsible computer users and network operators make use of anti-virus applications such as the F-Secure™ Anti-Virus product. For network operators, an optimal solution is to install an anti-virus application on individual client computers to scan data created and installed locally (e.g. from a floppy or CD-ROM drive, and an anti-virus application at the e-mail gateway to the network to scan e-mails and their attachments prior to their entry to (and possibly exit from) the network. Anti-virus applications may also be located at other locations. In the case of an anti-virus application located at an e-mail gateway, if a virus is detected in an e-mail and/or e-mail attachment, the e-mail and/or attachment may be disinfected if possible and forwarded to the recipient within the network or, if disinfection is not possible, the e-mail and/or e-mail attachment may be either quarantined or deleted and an appropriate notification sent to the recipient and network administrator.

Anti-virus applications typically make use of a database of virus signatures or fingerprints. Data is scanned by the application for the presence of these signatures. The providers of anti-virus applications are constantly seeking to identify new viruses

and to create signatures for these. Following the discovery of a new virus and the generation of a signature for that virus, the damage caused by that virus can be reduced by getting the signature into the field as quickly as possible. The signatures are distributed to anti-virus applications in the field using a number of techniques. Originally, signature updates were provided by posting out floppy disks or CD-ROM disks. However, the most common techniques used today employ Internet based protocols.

Statement of the Invention

Despite the best efforts of anti-virus product providers, it can sometimes take several hours or even a few days to generate a signature for a new virus following the discovery of that virus. This presents a window of opportunity for the virus to spread. In order to close this window, some administrators of vulnerable networks have in the past "manually" shut down their e-mail gateways following the issuing of a virus warning, until such time as a virus signature has been provided to them by their anti-virus product provider. It will be appreciated that this action often comes too late to avoid the infection of a network and the resulting damage.

According to a first aspect of the present invention there is provided a method of preventing the infection of a computer network by a computer virus, where that virus can be spread by e-mail traffic, the method comprising:

installing at an e-mail gateway of the network an anti-virus application, which application scans at least incoming e-mail traffic for known viruses;

in the event that a new virus is detected by the provider of the anti-virus application, sending a notification of this event from the provider to the anti-virus-application; and

at the anti-virus application, responding to said notification by failing to deliver incoming e-mails or their attachments to their recipients within the network and causing these e-mails or attachments to be re-directed to a buffer for safe storage.

Embodiments of the present invention provide a mechanism for rapidly "sealing" networks against viruses following the discovery of a new virus by an anti-virus product

provider. This minimises exposure of networks to infection prior to the generation and distribution of a signature for the virus.

There are a number of means by which anti-virus applications may be notified of the discovery of a new virus. Notifications may be pushed to the applications using IP (Internet Protocol) based protocols, e.g. HTTP or SNMP protocol, or using an Internet mechanism such as Backweb™, or may be pulled by the applications from a central server of the provider again using HTTP, e.g. the application may make a regular connection to a web site operated by the provider and at which virus alerts are made available. At least in the case of push mechanisms, notifications must contain some means for authenticating the origin of the message. This may be achieved using public/private key pairs. Some mechanism should also be available for enabling the provider to confirm that a notification has been received by a client.

Following the generation of a signature for the virus by the anti-virus application provider, and the provision of that signature to the application, the application may be arranged to scan the previously buffered e-mails or attachments for the virus. E-mails or attachments which are virus free are then delivered to their recipients. E-mails or attachments containing the virus, or suspected to contain the virus, are disinfected, quarantined or deleted, or are delivered to their recipients without attachments. Newly received e-mails may be scanned as normal using the updated signature database.

The application may check each signature update received from the provider to see if it contains a signature for said new virus. If so, then the application may proceed with said scan of the buffered e-mails or attachments and will scan newly received e-mails as normal. Alternatively, a separate notification may be sent from the provider to the application to notify the application that the latest signature update contains a signature for said new virus, and that the temporary e-mail diversion procedure can be terminated following installation of the latest update.

In certain embodiments, receipt of said first mentioned notification by the application may cause subsequently received e-mails to be delivered to their recipients minus any attachments. A copy of these e-mails with attachments are stored in the buffer.

According to a second aspect of the present invention there is provided an anti-virus application for installation on a network server on which is also installed an e-mail gateway, the application being arranged to interact with the e-mail gateway to scan incoming e-mails and/or e-mail attachments for known viruses, the application having means for receiving a notification from the provider of the application which notification causes the application to prevent delivery of e-mails or e-mail attachments received at the gateway and to divert these e-mails or attachments to a buffer for safe storage, and means for subsequently receiving a second notification from the provider which notification causes the application to cease preventing delivery of newly received e-mails or attachments.

According to a third aspect of the present invention there is provided a computer software storage medium having stored thereon an anti-virus application for causing a computer operating as an e-mail gateway to scan incoming e-mails and/or e-mail attachments for known viruses,

the application being arranged to receive a notification from the provider of the application which notification causes the application to prevent delivery of e-mails or e-mail attachments received at the gateway and to divert these e-mails or attachments to a buffer for safe storage, and to subsequently receive a second notification from the provider which notification causes the application to cease preventing delivery of newly received e-mails or attachments.

According to a fourth aspect of the present invention there is provided a method of preventing the infection of a computer network by a computer virus, where that virus can be spread by e-mail traffic, the method comprising:

installing at an e-mail gateway of the network an anti-virus application, which application scans at least incoming e-mail traffic for known viruses using a database of virus signatures;

in the event that a new virus is detected by the provider of the anti-virus application, calculating a checksum for the file carrying the virus or a relevant part of that file, and sending a notification containing the checksum from the provider to the anti-virus-application; and

at the anti-virus application, using the checksum to screen e-mails and/or their attachments for the virus until such time as a signature for the virus is received by the e-mail gateway from the application provider.

Brief Description of the Drawings

Figure 1 illustrates schematically a corporate LAN coupled to the Internet;
Figure 2 illustrates schematically an e-mail gateway of the corporate LAN of Figure 1; and
Figure 3 is a flow diagram illustrating a mechanism implemented at the e-mail gateway of Figure 2 for preventing virus infection of the corporate LAN.

Detailed Description of a Preferred Embodiment

There is illustrated in Figure 1 a corporate Local Area Network (LAN) 1 comprising a network backbone 2, a multiplicity of client work stations 3 and a plurality of servers including a network server 4 providing file storage capacity, an Internet server 5 for enabling the client workstations 3 to access the Internet 6, and an e-mail server 7. Both the Internet server 5 and the e-mail server 7 are coupled to the Internet 6 via a router 8.

The e-mail server 7 consists of a workstation running an e-mail server application such as Microsoft Exchange Server™, and having an "always connected" Internet connection. In use, the e-mail server application connects to a service provider 9 via the Internet 6 (using the SMTP protocol) to collect e-mails from and to deliver e-mails to the service provider 9. An anti-virus application, or anti-virus "gateway", is installed on the e-mail server 7. The application makes use of a database of signatures corresponding to known viruses. The database is updated using for example Backweb™ technology which causes updates to be pushed to the application from a central server 10, coupled to the Internet 6 via a router 16 and maintained by the application provider 15 (the application provider maintains in the server 10 a record of registered users to whom updates should be sent, together with their respective IP addresses or domain names). The anti-virus application incorporates web server functionality, having port TCP/IP 80 permanently open to allow HTTP connections to be established to the application by the central server 10.

The software architecture of the e-mail server 7 is illustrated schematically in Figure 2 where the e-mail server application and the anti-virus application are identified by reference numbers 11 and 12 respectively. Also shown in Figure 2 is a memory buffer 13 which may be provided by a portion of the hard disk space of the workstation on which the e-mail server is installed.

In normal use, when an e-mail is received by the e-mail server 7 from the service provider 9, delivery of the e-mail to the recipient is delayed and the e-mail scanned for viruses using the current virus signature database available to the anti-virus application 12. Typically, this might involve first determining whether or not the e-mail contains an attachment and, if so, scanning the attachment for viruses. In the event that no viruses are found, the e-mails and any attachments are delivered to the recipient client workstations 3. If a virus is found or is suspected to be present, the e-mail and its attachment is placed in a buffer memory. An attempt may be made to disinfect the e-mail. If the attempt is successful the mail and its attachment may be delivered to the recipient workstation. If it is unsuccessful, the mail and its attachment may be deleted, and a notification sent to the network administrator. Alternatively, the mail may be sent to the recipient with the attachment deleted.

As has been set out in the Background to the Invention section, there may be a significant delay between the discovery of a new virus and the generation and distribution of a signature for that virus. In order to minimise this window of opportunity during which e-mails can spread, a remote control feature is introduced into the anti-virus application 12. This allows the application provider to remotely control the e-mail server 7 to seal the server against infected e-mail traffic. The application 12 contains a mechanism which, when triggered remotely, instructs the e-mail server application 11 to divert incoming e-mails into a buffer 13 (e-mail servers typically already include an appropriate redirection mechanism, e.g. SMTP proxy). The e-mails are stored securely in this buffer until such time as a signature for the new virus is available and installed in the virus signature database of the application 12.

When a new virus is detected by an operator of the application provider and is deemed by that operator to be a high risk virus, the operator uses a web browser on his terminal

14 to establish an HTTP connection with each anti-virus application registered with the provider (in practice an instruction sent from the web browser to a filter at the server 10 results in a multi-cast operation being carried out by the server to establish the necessary multiple HTTP connections to port 80 of the web servers incorporated into the anti-virus applications, using the registered IP addresses or domain names). Once the HTTP connections are established, appropriate notifications are transmitted to the anti-virus applications. An ID code for the new virus will be included in the notifications. It will be appreciated that a firewall incorporated into the web servers can be used to authenticate and authorise the HTTP connections, and to prevent unauthorised access to the anti-virus applications.

When the anti-virus application 11 next receives a virus signature update (this may be pushed to the application from the application provider's server 10 or pulled by the application from that server 10), the application checks whether or not the update includes a signature for the new virus (which triggered the e-mail diversion mechanism) using the stored ID code for that virus. If the update does not contain the appropriate signature, the diversion mechanism is maintained. If on the other hand the update does include the appropriate signature, following the updating of the signature database, the application 11 scans the e-mails (and their attachments) using the updated database. E-mails certified as being virus free are released for delivery to their recipients within the LAN 1. E-mails which contain a virus (or which are suspected of containing a virus) are maintained in the buffer 13 or deleted, or held in quarantine by the anti-virus application. The e-mail server application 11 is then instructed to terminate the diversion mechanism and to resume normal delivery of the e-mails within the LAN (subject of course to the normal virus scanning procedure).

Figure 3 is a flow diagram further illustrating the anti-virus protection procedure described above.

It will be appreciated by the person of skill in the art that various modifications may be made to the above described embodiments without departing from the scope of the present invention. For example, protocols other than HTTP may be used to communicate between the anti-virus application provider and the anti-virus application. For example, a custom protocol using TCP/IP may be designed and used.

In another modification to the invention, following discovery of a new virus by the provider of the anti-virus application, the provider sends a notification to subscribing e-mail gateways containing a checksum for the file containing the virus (or a relevant part of that file). A checksum can be calculated extremely quickly for a new virus, as compared to the time taken to generate a virus signature, and so the notification can be sent to e-mail gateways within a few minutes or a few hours of the detection of the virus. Upon receipt of the notification, a gateway begins calculating a checksum for newly received e-mails and/or attachments, and compares the calculated checksums against the checksum contained in the notification. If a calculated checksum matches the notified checksum, the associated email or its attachment is quarantined or discarded. Whilst this approach does not guard against polymorphic viruses which change upon replication, it will guard against the majority of viruses. The use of a checksum to detect a virus is a relatively time consuming operation (on the part of the e-mail gateway), so as soon as a virus signature has been determined for the virus by the provider, this is sent to the e-mail gateways for incorporation into respective signature databases and the use of the checksum is terminated.

Claims

1. A method of preventing the infection of a computer network by a computer virus, where that virus can be spread by e-mail traffic, the method comprising:

installing at an e-mail gateway of the network an anti-virus application, which application scans at least incoming e-mail traffic for known viruses;

in the event that a new virus is detected by the provider of the anti-virus application, sending a notification of this event from the provider to the anti-virus-application; and

at the anti-virus application, responding to said notification by failing to deliver incoming e-mails or their attachments to their recipients within the network and causing these e-mails or attachments to be re-directed to a buffer for safe storage.

2. A method according to claim 1 and comprising establishing a communication channel between the anti-virus application provider and the anti-virus application using a TCP/IP or UDP/IP protocol, and sending said notification over said channel.

3. A method according to claim 1, wherein said notification is sent from the application provider to the application as an e-mail.

4. A method according to any one of the preceding claims, wherein said notification is sent from the application provider to the application as a result of a result of a request or enquiry sent from the application to the provider.

5. A method according to any one of the preceding claims, wherein, following the generation of a signature for the virus by the anti-virus application provider and the provision of that signature to the application, the application is arranged to scan the previously buffered e-mails or attachments for the virus, to deliver e-mails or attachments which are virus free to their recipients, and to cause the normal handling of e-mails at the e-mail gateway to be resumed.

6. An anti-virus application for installation on a network server on which is also installed an e-mail gateway, the application being arranged to interact with the e-mail

gateway to scan incoming e-mails and/or e-mail attachments for known viruses, the application having means for receiving a notification from the provider of the application which notification causes the application to prevent delivery of e-mails or e-mail attachments received at the gateway and to divert these e-mails or attachments to a buffer for safe storage, and means for subsequently receiving a second notification from the provider which notification causes the application to cease preventing delivery of newly received e-mails or attachments.

7. A computer software storage medium having stored thereon an anti-virus application for causing a computer operating as an e-mail gateway to scan incoming e-mails and/or e-mail attachments for known viruses,

the application being arranged to receive a notification from the provider of the application which notification causes the application to prevent delivery of e-mails or e-mail attachments received at the gateway and to divert these e-mails or attachments to a buffer for safe storage, and to subsequently receive a second notification from the provider which notification causes the application to cease preventing delivery of newly received e-mails or attachments.

8. A method of preventing the infection of a computer network by a computer virus, where that virus can be spread by e-mail traffic, the method comprising:

installing at an e-mail gateway of the network an anti-virus application, which application scans at least incoming e-mail traffic for known viruses using a database of virus signatures;

in the event that a new virus is detected by the provider of the anti-virus application, calculating a checksum for the file carrying the virus or a relevant part of that file, and sending a notification containing the checksum from the provider to the anti-virus-application; and

at the anti-virus application, using the checksum to screen e-mails and/or their attachments for the virus until such time as a signature for the virus is received by the e-mail gateway from the application provider.

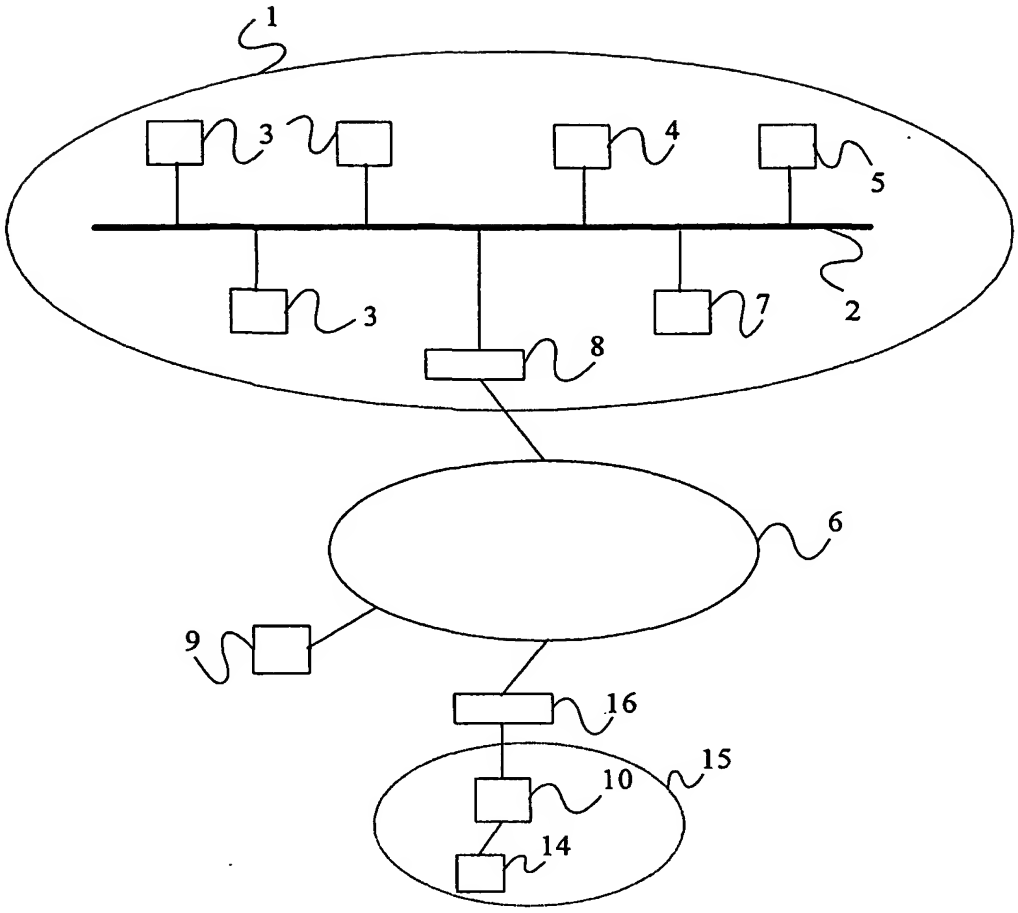


Figure 1

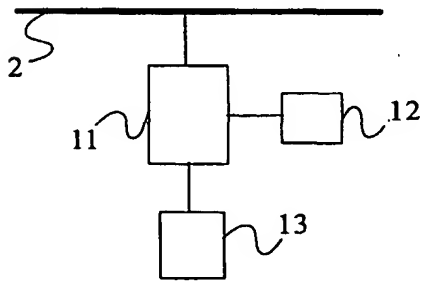


Figure 2

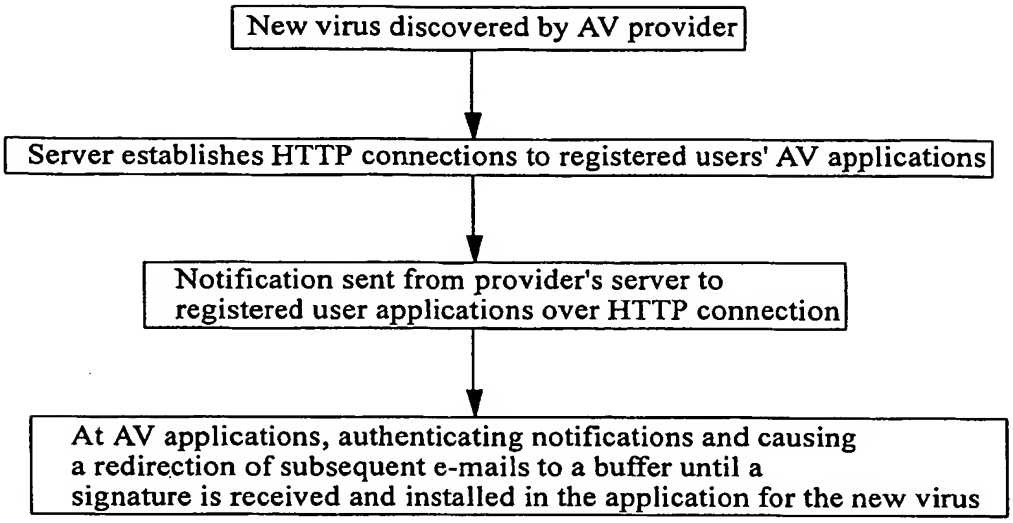

New virus discovered by AV provider
Server establishes HTTP connections to registered users' AV applications
Notification sent from provider's server to registered user applications over HTTP connection
At AV applications, authenticating notifications and causing a redirection of subsequent e-mails to a buffer until a signature is received and installed in the application for the new virus

Figure 3

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 July 2003 (31.07.2003)

PCT

(10) International Publication Number
WO 2003/063431 A3

(51) International Patent Classification[7]: H04L 12/58, 29/06

(21) International Application Number: PCT/EP2003/000752

(22) International Filing Date: 23 January 2003 (23.01.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0201648.3 25 January 2002 (25.01.2002) GB

(71) Applicant *(for all designated States except US)*: **F-SECURE OYJ** [FI/FI]; Tammasaarankatu 7, PL 24, Helsinki, FIN-00180 Helsinki (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LAHTI, Pasi** [FI/FI]; Stuurenkatu 5 A 20, FIN-00510 Helsinki (FI).

(74) Agents: **MARKS & CLERK** et al.; 4220 Nash Court, Oxford Business Park South, Oxford, Oxfordshire OX4 2RU (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

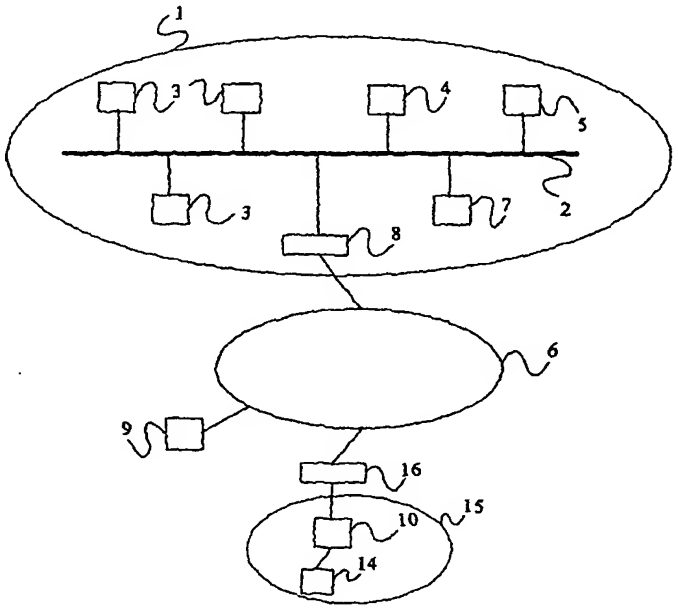
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
25 March 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ANTI-VIRUS PROTECTION AT A NETWORK GATEWAY



(57) Abstract: A method of preventing the infection of a computer network 1 by a computer virus, where that virus can be spread by e-mail traffic. The method comprises installing at an e-mail gateway 7 of the network an anti-virus application 12, which application scans at least incoming e-mail traffic for known viruses. In the event that a new virus is discovered by the provider of the anti-virus application 12, a notification of this event is sent from the provider to the anti-virus-application 12. At the anti-virus application 12, receipt of said notification results in the diversion of incoming e-mails or their attachments to a buffer 13 for safe storage.

WO 2003/063431 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/00752

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/58 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MICROWORLD: "Security on the Gateways" WHITE PAPER, [Online] 2000, pages 1-7, XP002245105 Retrieved from the Internet: <URL:http://www.mwti.net/pdfs/whitepaper1_mailscan.PDF> [retrieved on 2003-06-20] abstract page 5, line 1 - page 7, line 2 -----	1,6,7
A	US 5 889 943 A (TSAI WARREN ET AL) 30 March 1999 (1999-03-30) abstract -----	1,6,7

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 June 2003	14 10. 2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Nocentini, I.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP 03/00752

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-7

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-7

A method of remotely suspending the delivery of new incoming e-mails when a new virus is discovered.

---

2. claim: 8

A method for finding new viruses using the checksum of an infected file.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 03/00752

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5889943 A	30-03-1999	US 5623600 A	22-04-1997
		AU 2556697 A	07-11-1997
		EP 0954794 A2	10-11-1999
		JP 2000517440 T	26-12-2000
		WO 9739399 A2	23-10-1997
		AU 2001997 A	17-04-1997
		DE 19680539 T0	11-12-1997
		EP 0852762 A1	15-07-1998
		GB 2309561 A	30-07-1997
		JP 11513153 T	09-11-1999
		WO 9712321 A1	03-04-1997